МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
Высшего образования
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ МОРСКОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Кафедра судовой автоматики и измерений

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Разработка эмулятора протокола квантового распределения ключей с использованием парадокса Эйнштейна-Подольского-Розена

Выполнил студент: Соколов Г.А.
Группа: 2450
Проверил: к.т.н., доцент: Шавинская С.К.

Цель работы

{Разработка программного эмулятора протокола квантового распределения ключей с использованием парадокса ЭПР.}

ИНСТРУМЕНТЫ:

Python 3.12

Сторонние библиотеки: ***qutip, numpy, pandas, random, matplotlib, hashlib, warnings***

- **– GraphPad**: инструмент для визуализации данных. Полученные в ходе экспериментов данные были экспортированы и далее обработаны в программе GraphPad для улучшения визуального представления данных и более детального анализа.
- **– Pycharm IDE**: среда разработки, в которой происходило создание кода.
- **– Excel**: используется для хранения и анализа результатов тестов. С помощью библиотеки pandas данные записываются в Excel-файлы.

Проблема распределения ключа в криптографии

	Симметричное шифрование	Асимметричное шифрование
Ключ	1 ключ	2 ключа
Скорость	Высокая (аппаратное)	Ниже (более сложные мат. Операции)
Распространение ключа	Требуется	Не требуется
Примеры:	AES, DES, 3DES	RSA, ECC, DSA
Уязвимость	Менее уязвимы к атакам, основанным на квантовых вычислениях, т.к. ускорение может быть скомпенсировано удлиннением ключа. **Алгоритм Гровера ускоряет подбор ключа длиной n в $\sqrt{n}$ раз:** $2^{\frac{256}{2}} = 2^{128}$	Квантовый алгоритм Шора и подобные может разрушить безопасность RSA, ECC и других асимметричных алгоритмов _____ (P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994)
Повышение безопасности	Сопоставимое увеличение ресурсоёмкости атаки может быть достигнуто удлинением длины ключа _____ **NIST, "Report on Post-Quantum Cryptography," April 2016**	постквантовые алгоритмы, обеспечивающие более высокую математическую защиту (например, на основе решёток или изогений эллиптических кривых)

Квантовая запутанность: парадокс ЭПР

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

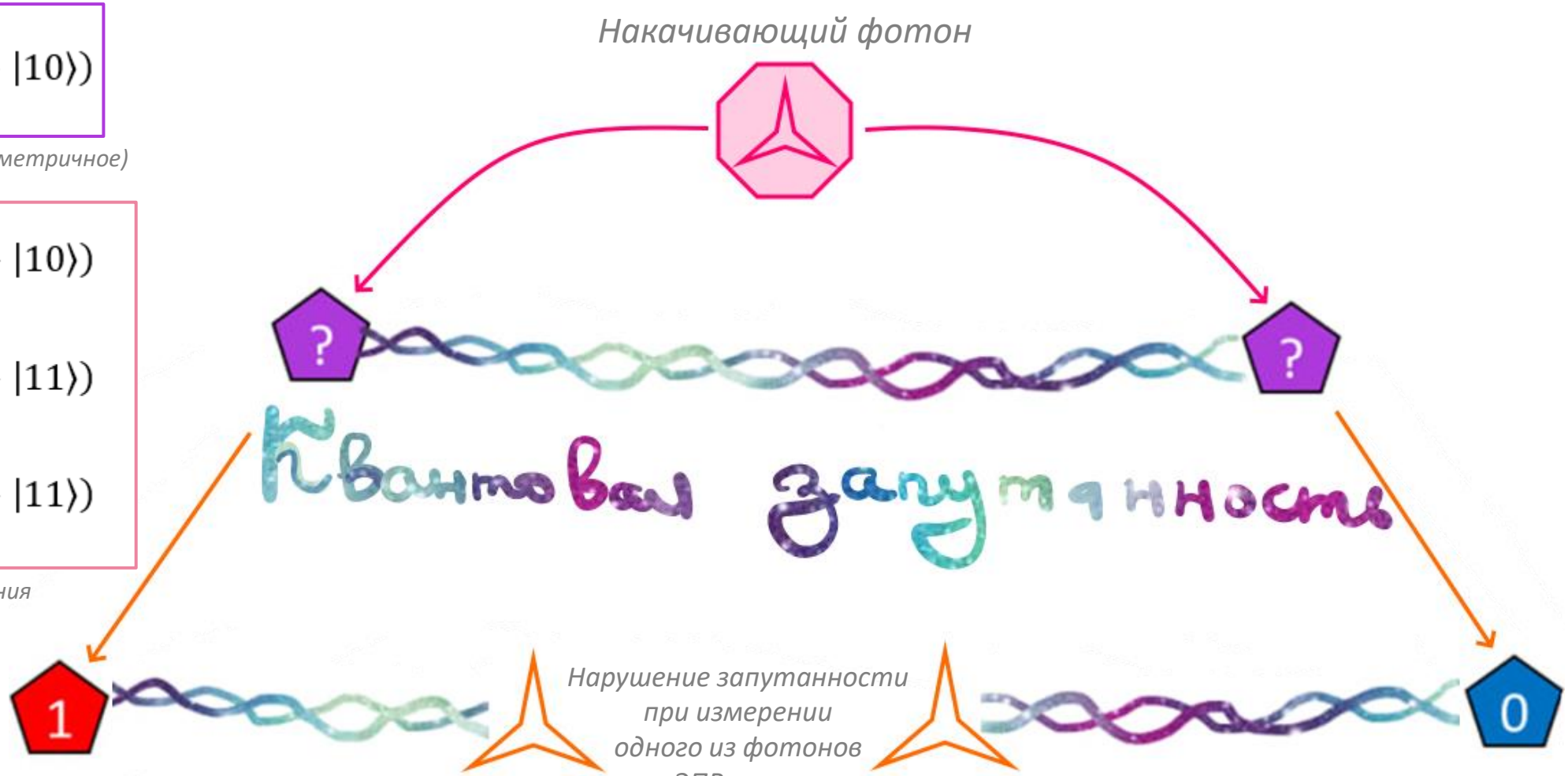
Синглетное состояние (асимметричное)

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

Триплетные состояния (симметричные)



Классический предел

$$S = |E(a,b) - E(a,b') + E(a',b) + E(a',b')|$$

неравенство CHSH *(Clauser-Horne-Shimony-Holt)*

$$A(a,\lambda)$$
$$B(b,\lambda)$$

A, B = +1 или -1 зависят от скрытых переменных

$$E(a,b) = \int d\lambda p(\lambda)\, A(a,\lambda)B(b,\lambda)$$

$$S = \left|\int d\lambda p(\lambda) \left[\begin{matrix} A(a,\lambda)B(b,\lambda) - A(a,\lambda)B(b',\lambda) + \\ +A(a',\lambda)B(b,\lambda) + A(a',\lambda)B(b',\lambda) \end{matrix}\right]\right|$$

$$\left|\begin{matrix} A(a,\lambda)B(b,\lambda) - A(a,\lambda)B(b',\lambda) + \\ +A(a',\lambda)B(b,\lambda) + A(a',\lambda)B(b',\lambda) \end{matrix}\right| \leq 2$$

$$S = E(a,b) - Ea,b' + Ea',b + E(a',b') \leq 2$$

Классический предел

Квантовый предел

$$S = |E(a,b) - E(a,b') + E(a',b) + E(a',b')|$$

$$A(a,\lambda) \qquad B(b,\lambda)$$

A, B = +1 или -1 зависят от скрытых переменных

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$|\psi^-\rangle = -|\psi^-\rangle$$

Синглетное антисимметричное состояние с нулевым суммарным спином (состояние Бэлла)

Корреляционная в квантовой механике рассчитывается как ожидаемое значение продукта измерений на двух частицах:

$$E(a,b) = \langle\psi^-|\sigma_a \otimes \sigma_b|\psi^-\rangle$$

может быть выражена через углы поляризационных фильтров ***a*** *и* ***b:***

$$E(a,b) = \cos(2(a-b))$$

Подберём углы с максимальной суммой косинусов:

$$a = 0^\circ \qquad b = 22.5^\circ$$

$$a' = 45^\circ \qquad b' = -22.5^\circ$$

$$E(a,b) = \cos(2(0^\circ - 22.5^\circ)) = \cos(-45^\circ) = \frac{1}{\sqrt{2}} \approx 0.707$$

$$E(a,b') = \cos(2(0^\circ - (-22.5^\circ))) = \cos(45^\circ) = \frac{1}{\sqrt{2}} \approx 0.707$$

$$E(a',b) = \cos(2(45^\circ - 22.5^\circ)) = \cos(45^\circ) = \frac{1}{\sqrt{2}} \approx 0.707$$

$$E(a',b') = \cos(2(45^\circ - (-22.5^\circ))) = \cos(90) = 0$$

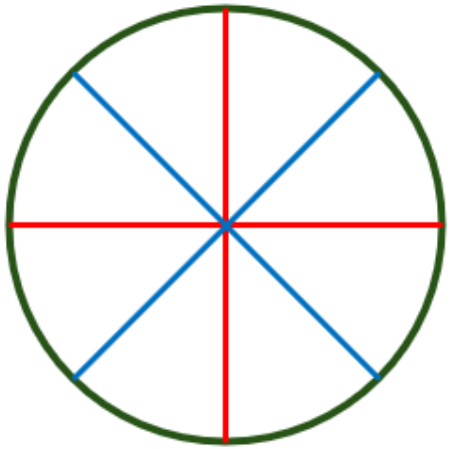
$$S = \left|\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + 0\right|$$

$$S = \left|0 + \frac{1}{\sqrt{2}}\right|$$

$$S = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = \frac{2}{\sqrt{2}} = \sqrt{2} + \sqrt{2} = \mathbf{2\sqrt{2}}$$

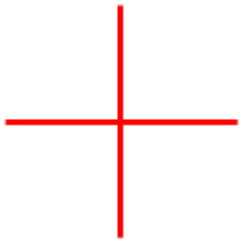
Квантовый предел

Базисы E91



E91

=



Линейный Базис

$(|0\rangle)$

$(|1\rangle)$

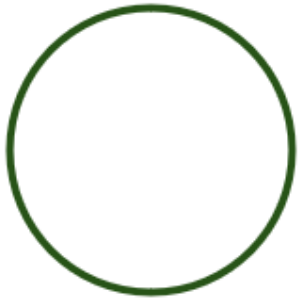
+

Диагональный Базис

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

+



Круговой Базис

$$|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

$$|L\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

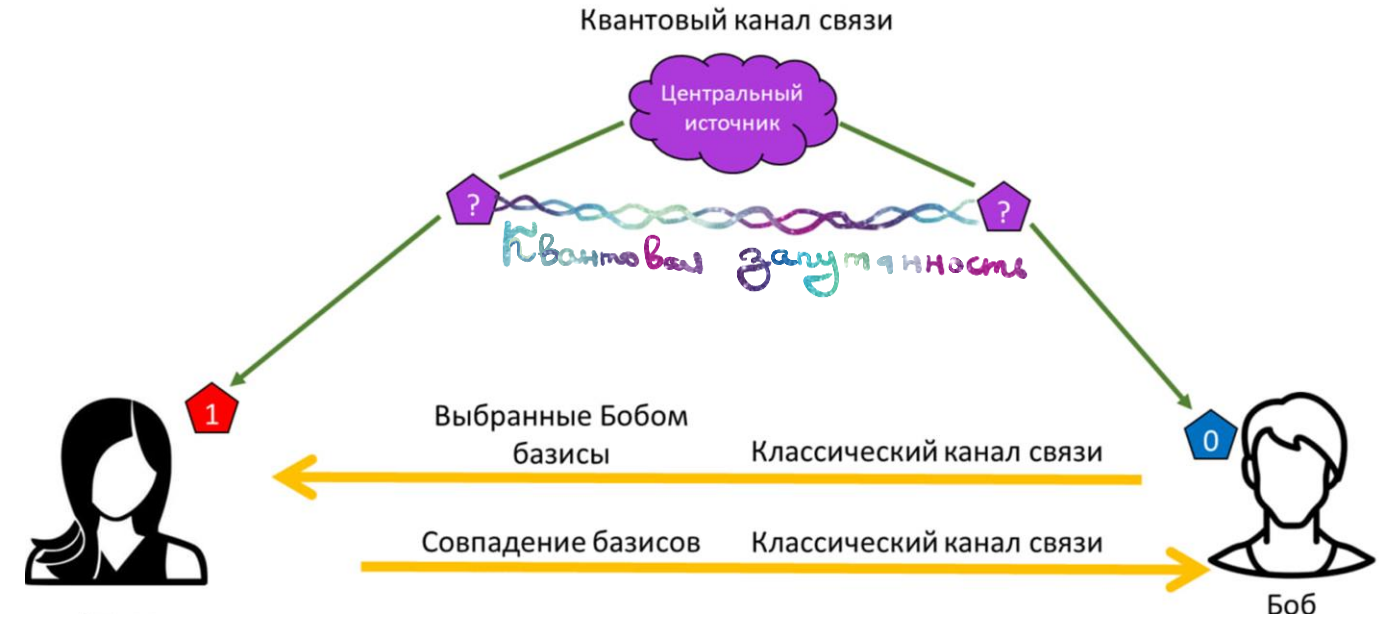
Состояние	⇔	⇕	⤢	⤡	↻	↺
Кубит	0	1	0	1	0	1

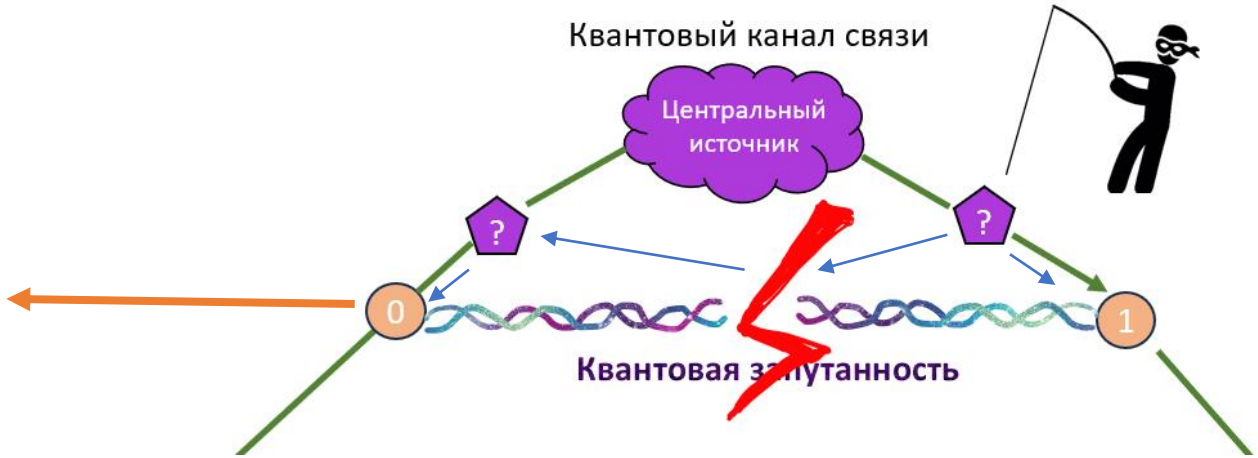
QKD протокол E91

Состояние	⇔	⇕	⤢	⤡	↻	↺
Кубит	0	1	0	1	0	1

№ ЭПР пары	1	2	3	4	5	6	7	8	9	10	11	12	…	n
Генерация и распределение ЭПР пары – квантовый канал														
Базисы Алисы	+	+	x	o	x	x	o	+	o	x	o	+	…	x
Базисы Боба	+	x	x	+	x	+	o	+	+	o	o	x	…	x
Значения Алисы	1	1	0	0	0		0	1			1	0	…	1
Значения Боба	0	1	1	1	1		1	0			0	0	…	0
Сверка Базисов – классический канал														
=	=		=		=		=	=			=		…	=
Проверка выполнения неравенства Белла (QUBERT)														
Итоговый ключ	1		0		0		0	1			1		…	1

Методы постобработки
(коррекция ошибок, повышение конфиденциальности)





Разработка эмулятора E91

1. Реалистичные запутанные состояния (qutip)

```python
# Функция для генерации запутанных пар
1 usage
def generate_entangled_pairs(num_pairs):
    psi = bell_state('00')  # Запутанное состояние Белла
    return [{"id": i, "state": psi, "entangled": True} for i in range(num_pairs)]
```

2. Шум

```python
# Шум (0.1% вероятность)
1 usage
def noise(pair):
    if pair['entangled'] and np.random.random() < 0.01:
        pair['state'] = (random.randint( a: 0,  b: 1), 1 - random.randint( a: 0,  b: 1))
        pair['entangled'] = False
        return True
    return False
```

3. QBER (Quantum Bit Error Rate)

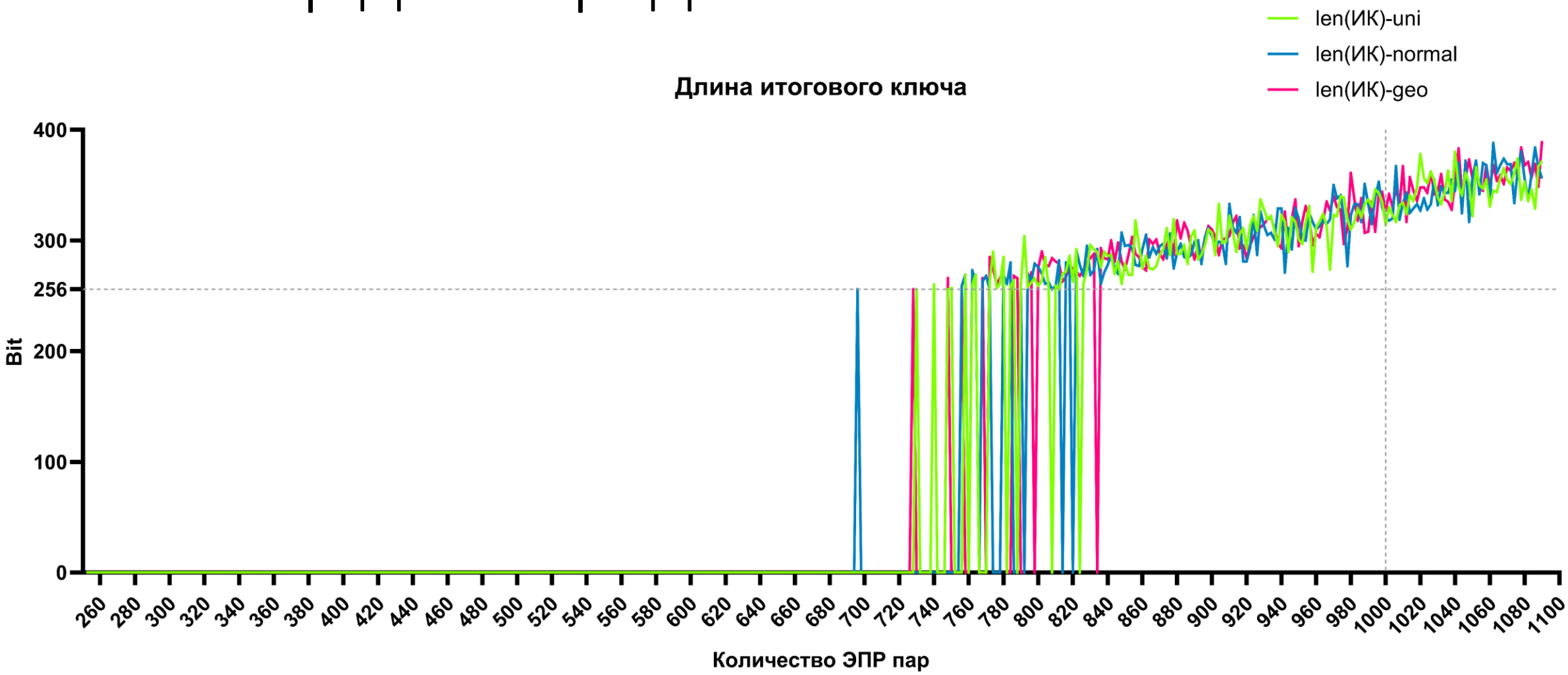
```python
# Расчет QBER
1 usage
def calculate_qber(alice_key, bob_key, num_pairs):
    errors = sum(1 for a, b in zip(alice_key, bob_key) if a == b)
    return errors / len(alice_key)
```

Разработка эмулятора E91: генерация вероятностей перехвата с заданным типом распределения

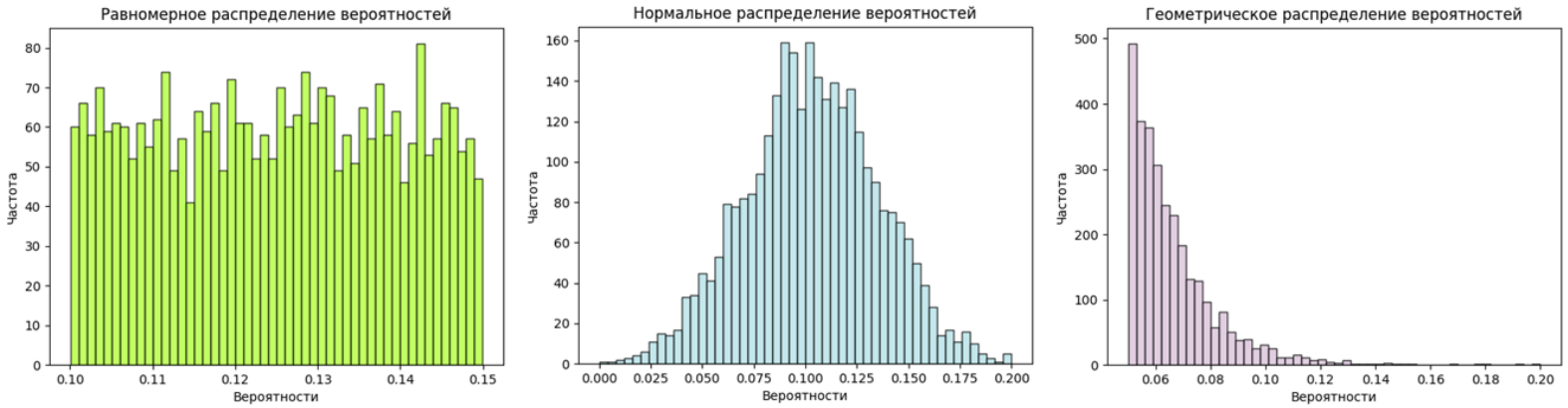
```python
if model_name == 'Равномерное':
    # Параметры равномерного распределения
    a, b = 0.1, 0.15  # Диапазон значений от 0 до 0.15
    # Генерация равномерного распределения
    probabilities = np.random.uniform(a, b, num_tests)
elif model_name == 'Нормальное':
    # Параметры нормального распределения
    mean = 0.5  # Пик нормального распределения
    std_dev = 0.05
    # Генерация нормального распределения
    probabilities = np.random.normal(mean, std_dev, num_tests)
    probabilities = (probabilities - np.min(probabilities)) / (
            np.max(probabilities) - np.min(probabilities)) * 0.2 * k
elif model_name == 'Геометрическое':
    # Параметр геометрического распределения
    p = 0.01  # вероятность события
    # Генерация геометрического распределения
    probabilities = np.random.geometric(p, num_tests)
    probabilities = (probabilities - np.min(probabilities)) / (
        np.max(probabilities) - np.min(probabilities)) * 0.15 + 0.05
```

```
ТЕСТ params #3.1
ДИНАМИЧЕСКАЯ ВЕРОЯТНОСТЬ - Геометрическое распределение
- - - - - - - - - - - - - -
// unique probability line generated... ChartDisplaying is off due to direct script call

[0.06625    0.05       0.07375    0.0675     0.07416667 0.0725
 0.06083333 0.07166667 0.08291667 0.1        0.07375    0.07666667
 0.05416667 0.07291667 0.05125    0.05166667 0.12708333 0.06583333
 0.10916667 0.05041667 0.125      0.05875    0.08583333 0.08916667
 0.05166667 0.08166667 0.08208333 0.05875    0.08375    0.06833333
 0.05791667 0.05541667 0.09666667 0.11083333 0.09916667 0.0575
 0.2        0.09125    0.16666667 0.06333333]
Ключи Алисы и Боба инвертны

Длина итогового чистого ключа недостаточна: 12, реинициализируйте протокол
Присутствие криптоаналитика не обнаружено:  QUBER = 0%
```

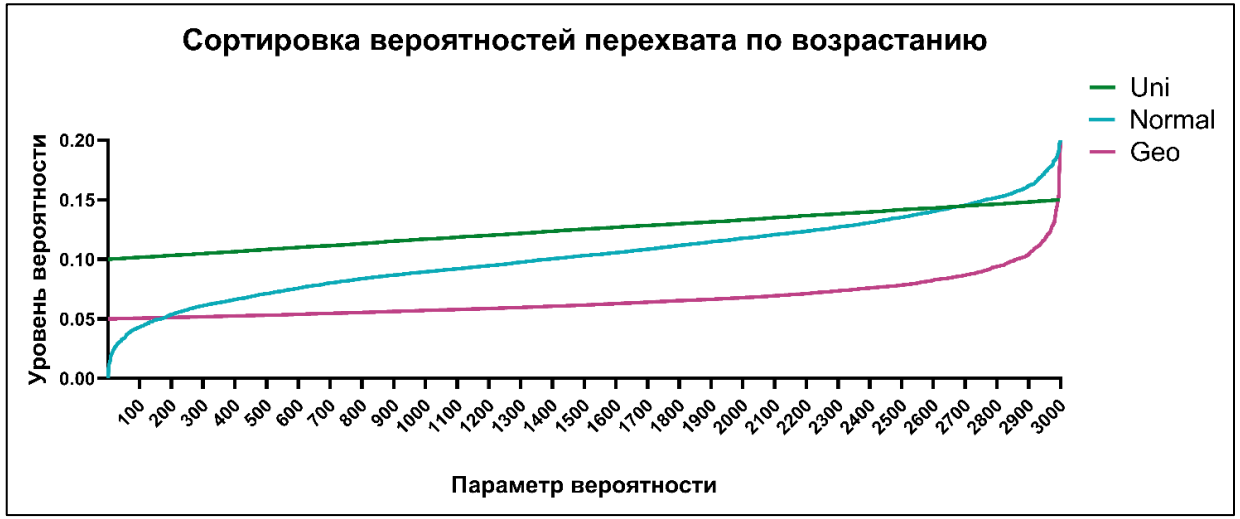
Определение оптимального количества ЭПР пар для передачи



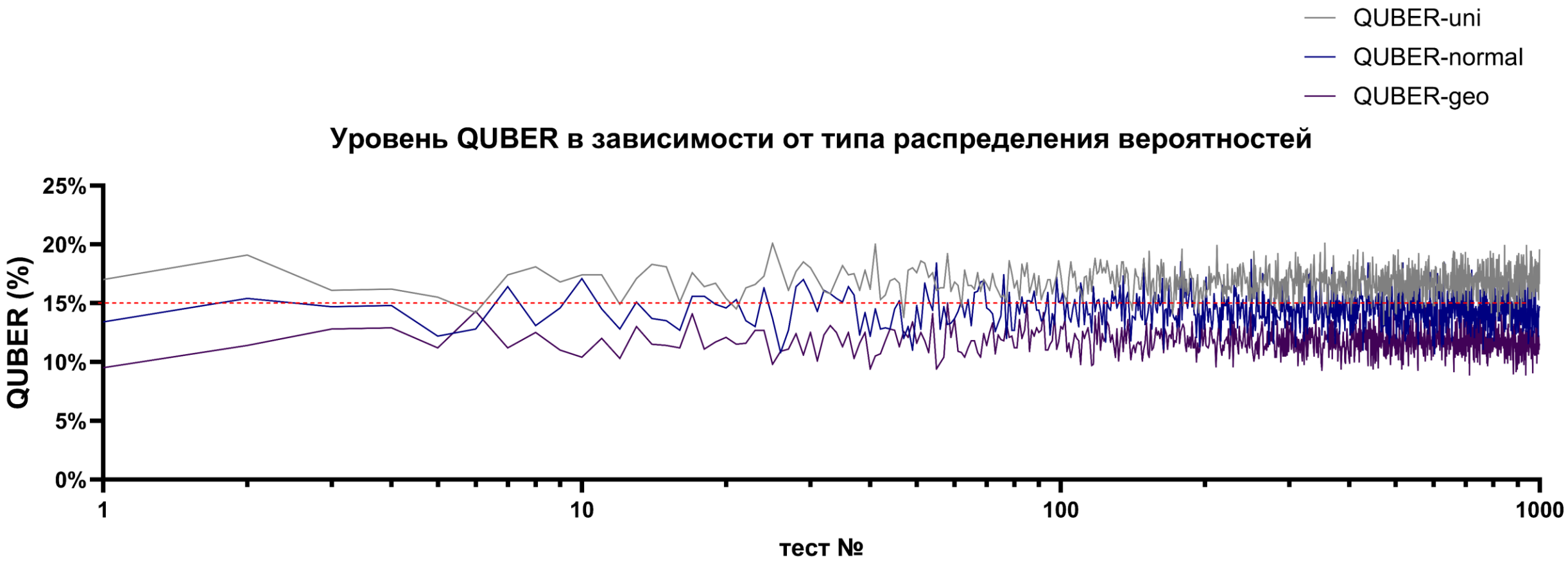
Проверка корректности генерации ряда вероятностей



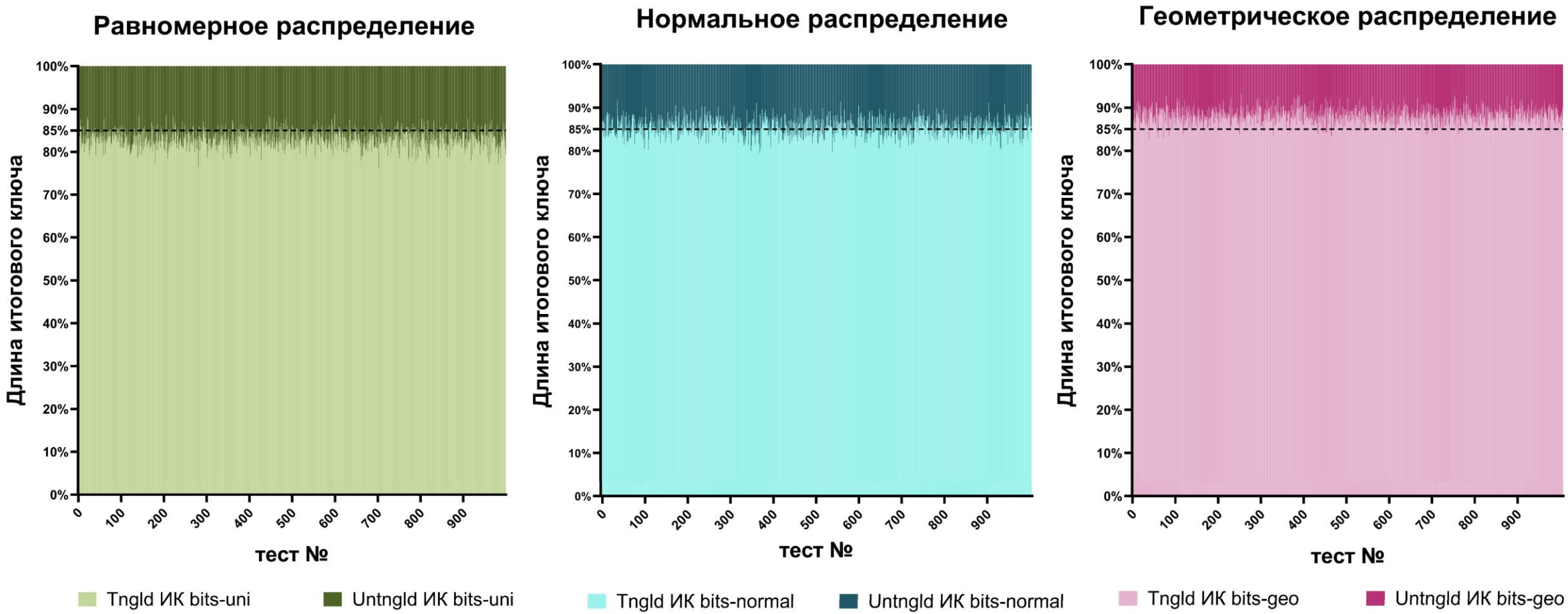
Сгенерированные распределения вероятностей



Тестирование корректности генерации рядов вероятностей в соответствии с заданным распределением



Состав итогового ключа: запутанные и незапутанные биты



Дальнейшие векторы улучшения

- Специальные квантовые библиотеки
- Спектр атак и сценарии
- Эмуляция шумов с использованием объективных математических моделей:
  - Потери квантовых состояний
  - Шумы и декогеренция
  - Дисперсия и искажения

- Чистый генератор случайных чисел
- Учёт погрешности детекторов
- Другие способы перехвата

- Дополнительные методы постобработки

Заключение

- *Разработан программный эмулятор протокола E91*

- Проведены тесты для определения поведения эмулятора при различных заданных типах распределения вероятностей перехвата
- Проведён анализ результатов тестирования
- Определены дальнейшие векторы улучшения

{ Цели работы достигнуты. }

Спасибо за внимание!